Administrative Regulation 43
City of Portland Technology Use Policy

Overview:

The City of Portland provides employees with access to information technology resources to improve the quality and timeliness of work-related information. The intent of this administrative regulation is to guide proper usage of City of Portland information technology resources.

Applicability:

This policy applies to all users regardless of location when accessing or using the City's information technology resources.

Policy:

I. Definitions

Access – The ability to communicate using an information system.

Electronic Mail (e-mail) – The electronic transfer and storage of electronic data, documents and information in the form of electronic messages, memoranda, and attached documents to or from a sending party to one or more users via a telecommunication system.

Equipment – Computers, monitors, keyboards, mice, routers, switches, hubs, software, telephones, fax machines, photocopiers or any other information technology resource.

Information Technology Resources – Equipment, software or services used to input, store, process, transmit, and output information, including, but not limited to, desktops, laptops, mobile devices, servers, telephones, fax machines, copiers, printers, internet, email, and social media sites.

User – All City of Portland employees, elected officials, volunteers and any other persons providing services to the City or utilizing the City of Portland information technology resources.

II. Responsibilities

The responsibility for ensuring that City information technology resources are used safely, appropriately, and in compliance with this policy is shared between individual users, supervisors and department heads, and the IT Department.

User responsibilities – All users of the City's information technology resources are responsible for the following:

- Ensuring their own complete compliance with the provisions of this policy; and
- Staying informed of City information that is disseminated electronically, including understanding and keeping up-to-date on any changes to this policy.

Supervisors and Department Head responsibilities – Supervisors and Department Heads bear responsibility for the following with respect to City information technology resources:

- Distributing this policy and any updates to all direct reports and department employee, and ensuring that they understand expectations; and
- Ensuring that their direct reports and department employees comply with the provisions of this policy.

Information Technology Department – The IT Department management and staff are responsible for the following, as indicated:

- IT Department management will review and update this policy, as needed;
- IT Department management will continue to develop and publicize record keeping practices consistent with this policy in their area of responsibility including the routing, formatting, and filing of records communicated via e-mail;
- The IT Department network administrators and staff are responsible for e-mail security, backup, and disaster recovery;
- The IT Department will advise staff in appropriate use, including appropriate personal use of e-mail, and be responsible for ensuring the security of physical devices and passwords; and
- The IT Department, along with Corporation Counsel's Office will be available for assistance in complying with this policy.

III. No Expectation of Privacy

Emails, electronic files, and all other usage of information technology resources are not confidential, and no user has any expectation of privacy in that usage. The City of Portland reserves the right to examine, monitor, and regulate usage of information technology resources as a condition of being allowed to use those resources. The IT Department can, at the direction

of Corporation Counsel or the City Manager, review emails, files, and other activity using information technology resources.

The IT Department, in consultation with the City Manager and/or Corporation Counsel, further reserves the right to revoke access to information technology resources and to remove files and software that do not comply with this policy or otherwise are inappropriate or pose a danger to the City's resources.

IV. Acceptable Use Standards

The telephone, Internet, newsgroups, e-mail, and other information technology resources give City employees considerable reach to propagate information to describe City programs, services and policies. However, anything an employee communicates using information technology resources can be interpreted as representing the City of Portland. Further, access to the Internet could enable unauthorized external access to City data and networks if employees do not apply appropriate security.

For these reasons, when using City information technology resources, users must adhere to the following guidelines:

- Users may only use information technology resources for official City of Portland business, unless an exception is specifically granted by an employee's supervisor, in which case, an employee may use Internet access for non-business research or browsing during mealtime or other breaks or outside of working hours, provided that all other standards of this Policy and other City policies are adhered to;
- Users may not use information technology resources to solicit for causes unrelated to City business;
- Users may not share user IDs or passwords;
- Users must conduct themselves honestly and appropriately;
- Users must respect and not infringe upon any copyrights, software licensing rules, property rights and the privacy of others;
- Users may not intentionally violate any laws, ordinances, or regulations;
- Users may not use information technology resources to send or propagate messages that are defamatory or libelous;
- Users may not commit any violations of City policies, including, but not limited to misuse, theft, or misappropriation of City assets, committing harassment or discrimination, unauthorized release of confidential material, or other infractions;
- Users may not use information technology to display, access, store, distribute, edit, or record sexually explicit or pornographic material, unless use of such material falls within the user's legitimate job responsibilities, as previously approved by the City Manager or Corporation Counsel;
- Users may not access personal Internet Service Provider accounts over City networks, unless the access is for City related business;

- Users may not download software from the internet without first obtaining approval from the Information Technology Department;
- Users may not knowingly receive or propagate any virus, worm or any other form of malicious software;
- Users may not download or distribute pirated software or data;
- Users may not intentionally disable or overload any technology intended to protect the privacy or security of data; and
- Users may not upload to the Internet any software licensed by the City or data owned by the City without written authorization from the Information Technology Department.

V. Document Retention Requirements and Freedom of Access Requests

Emails, databases, and other electronic files are generally considered public records, which the City and all employees and elected officials have a responsibility to preserve and protect. Final versions of electronic files and databases should not be deleted or destroyed without first consulting with the IT Department or Corporation Counsel's Office.

With respect to emails, users must adhere to the following guidelines:

1. *Read* e-mails regularly.
2. *Delete* all e-mails that do NOT relate to your job functions with the City.
   Examples of what to delete: Personal e-mails; spam and junk; non-substantive e-mails such as those about farewell receptions, cake in the breakroom, health tips, lost keys, etc.
3. *Archive* all e-mails that relate to your job functions with the City.

Examples of what to save: Any e-mails concerning projects you are working on; City documents; contact with the public in your official capacity.

Due to the nature of Public Safety matters, Police and Fire Departments are responsible for developing and implementing internal electronic document policies consistent with this administrative regulation.

Many electronic documents, files, and emails are public records, subject to the Freedom of Access Act. However, you should not automatically turn over requested documents, unless you have previously received guidance to do so. If you or a member for your staff receives a request for access to or a copy of electronic files, you must contact the City's Freedom of Access Officer, currently Jessica Grondin, or Corporation Counsel's Office immediately for instructions.

VI. Confidentiality and Security

Maine statutes make certain records confidential, including (but not limited to) personnel files, criminal history records, patient information, and client information. These are not public

records, and the City and its employees, elected officials, and agents have an obligation to safeguard the confidentiality of such records. Users are individually responsible for maintaining the security and confidentiality of any confidential records that they might have access too. Downloading, emailing, faxing, accessing, sending, receiving, or otherwise using confidential records in any manner that is not specifically permitted in the context of the user's job functions is a violation of this policy. Absent express permission from the IT Department, the City Manager, and/or Corporation Counsel, confidential records may not be sent to a personal email address, downloaded on an external drive for removal from the City, or otherwise removed from City facilities.

Where confidential or sensitive information is saved or downloaded, it must be encrypted, password protected, or otherwise protected from access. Even where records or files are not confidential, users should not share or send such records where not otherwise authorized to do so, and the sharing and sending is not part of the user's duties with the City.

VII. Reporting Security Breaches

If any user becomes aware of a possible breach in administrative data or computer security they must report it to the IT Department immediately via email help@portlandmaine.gov.

Upon notification of a possible security breach the IT Department will investigate all facts related to the situation, consult with Corporation Counsel and any other relevant resources, and recommend a course of action to the appropriate Department Head and/or City Manager.

Policy Violations:

Any employee who is found by the City of Portland to have violated this policy will be subject to sanctions appropriate to the circumstances, ranging from a verbal warning up to and including dismissal. Violations subject to immediate dismissal include, but are not limited to, the intentional misuse or improper dissemination of confidential information; the intentional breach or compromise of the City's data or systems; and the loss or destruction of City property or equipment arising out of failure to follow this policy.

Any user who is found or suspected by the City of Portland to have violated this policy will be subject to having their access rights revoked, and any other available remedies that are appropriate, including criminal prosecution.

Signed by Jon Jennings

_____

Jon P. Jennings, City Manager

REV 11.6.18

Administrative Regulation 43
City of Portland Technology Use Policy

To be completed by all users of City information technology resources.

User Acknowledgement

I have read Administrative Regulation 43: City of Portland Technology Use Policy. I fully understand this policy and agree to abide by its terms. I specifically understand and agree that:

- The user identifier and password issued to me allowing access to City information technology resources are confidential and solely for my own use in carrying out my job responsibilities. I will not loan, divulge, or make this information available to anyone other than management.

- Files or programs I create for the City of Portland, on City time, or using City resources are the property of the City.

- The City reserves the right to review, audit, and inspect, at its discretion, files, emails, usage history, and other information created or accessed using City information technology resources, even if protected by my password.

- The unauthorized release or loss of City confidential information, intentionally breaching or allowing the breach of data, or other violations of this policy may subject me to consequences, including discipline or dismissal for employees, the revocation of user authority, criminal prosecution, and/or other penalties.

SEEN AND AGREED

_____ _____

Date User Signature

_____

User Name Printed